Axisサイバーセキュリティのフレームワークと実践

2025年1月、バージョン1.2

AXIS COMMUNICATIONS

目次

1. はじめに

情報、テクノロジー、セキュリティ業界の顧客にとっては、自社ビジネスに導入されるソリューションの安全性と信頼性を確保することが非常に重要です。システムとデータは、意図したユーザーのみがアクセス可能な状態に維持されている必要があります。また、侵入や不測の情報漏洩を心配せずに、デバイスをネットワークに接続して使用できる環境が整っていなければなりません。整合性が維持され、機能が中断されずに、設計および意図通りに機能するソリューションが必要なのです。

しかし、セキュリティ脅威は常に存在します。継続的に新たな脅威が発生し、いつ何時その性質が変化するか分かりません。

セキュリティ対策に真摯に取り組んでいるアクシスコミュニケーションズは、セキュリティと関連リスクに継続的に対処できるプロセスと手順を整えています。当社の従業員はすべて、セキュリティ意識向上および払うべき注意に関するトレーニングを受けています。

本文書を通して、Axisのサイバーセキュリティのフレームワークと実践の詳細をご紹介します。当社のフレームワークは、資産の機密性、整合性、可用性を保護する体系的なアプローチを実現できるように構成されています。

2. サイバーセキュリティのフレームワーク

サイバーセキュリティのフレームワークの基盤となっているのが、Axisの情報セキュリティマネジメントシステム（ISMS）です。ISO 27001:2023の要件に基づくこのISMSにより、Axisのセキュリティ体制の継続的な改善とフォローアップを促進することができます。ISMSは、証明書で定義された範囲についてISO 27001:2023の認証を取得しています。

ISMSの一環として、AxisはISO 27002の規格に基づくサイバーセキュリティ制御フレームワークを実装しています。ISO 27001への準拠を証明することを目的として、ISMSおよび関連するセキュリティ管理はいずれも、認定を受けた外部認証機関による監査を毎年受けています。Axisはまた、経営陣が決定した年間内部監査計画に従って、ISMSの内部監査を実施しています。

2.1 情報セキュリティポリシー

Axisの情報セキュリティポリシーには、Axisのセキュリティ管理の全体的な方向性が定められています。情報セキュリティポリシーは必須要素であり、すべての従業員、臨時労働者、コンサルタントだけでなく、経営陣と取締役もこれに遵守する必要があります。

当社はまた、ガイドライン、慣行、Axisセキュリティベースラインといったより詳細な関連文書によって情報セキュリティポリシーを補完しています（詳細については、第3章を参照してください）。情報セキュリティポリシーとその基礎となる文書は毎年見直され、Axisの全体的なビジネス戦略の変更や環境の変化に応じて更新されます。

2.2 役割と責任

セキュリティの継続的な改善を推進する役割が、組織全体に複数配置されています。セキュリティに対する協力的なアプローチを推進するAxisは、全従業員が重要な役割を担っていることを強調しています。セキュリティに特化した役割と組織の例として以下が挙げられますが、これらに限定されるものではありません。

> 最高情報責任者（CIO）
- Axisの情報セキュリティとプライバシーに対する総合的な責任を担います。
- 経営陣の一員として、セキュリティ関連事項について取締役会に報告する任務を負っています。

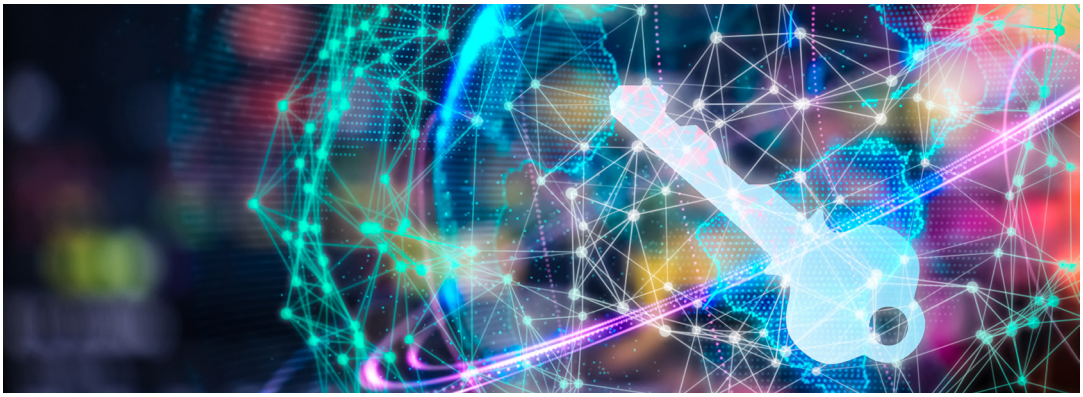
> ISMS管理部署
- ISMSの監督を行います。

> プライバシーコンプライアンス部署
- 社内のプライバシーに関する窓口となります。

> ITガバナンス
- Axis ISMSに関する方法論と構造を継続的に開発します。

> ソフトウェアセキュリティグループ（SSG）
- セキュリティ関連事項に関する開発組織の主要内部連絡機関です。
- より安全なソフトウェアを開発することを目的として、Axisの活動を定義するフレームワーク「Axisセキュリティ開発モデル（ASDM）」に対する責任を担います。
- ASDMは、ISMSに基づいて安全な開発を推進するコンポーネントです。

> セキュリティオペレーションセンター（SOC）
- 24時間年中無休でサイバー脅威の監視、検知、対応を行います。



3. Axisセキュリティベースライン

Axisセキュリティベースラインは、Axisにおけるセキュリティ要件の中心的なリファレンスであり、Axisの情報セキュリティポリシーの重要な要素です。

セキュリティベースラインを確立するため、Axisは世界的に認められているISO 27001/2やNIST SP 800-53などのセキュリティフレームワークおよびGDPRといった規制要件を参考にして、いくつかの領域を定義しています。以下は、それぞれの領域と適用される実践の概要です。

3.1 資産の管理と情報の分類

組織として、Axisにとって情報資産は非常に価値のあるものであり、これは適切に保護する必要があります。Axisは資産目録を維持し、資産をその重要度に基づいて分類して資産を管理しています。資産管理に関するガイダンスには、定義された分類レベルを備えた資産分類スキームが含まれます。資産の機密性、整合性、可用性を効率的に保護する上で、資産の分類は必須要件となります。

特定した資産に事業と技術の責任者を割り当て、資産目録に記載しています。責任を割り当てられた担当者が、資産目録と分類に関する作業を継続的に担います。

3.2 バックアップとリカバリ

バックアップとリカバリの手順は、データ損失を防ぎ、データを十分に復元できるように構成されています。データの可用性要件に応じて、バックアップが少なくとも毎日実行されています。そして、すべてのバックアップはセカンダリ バックアップ ストレージに記録されます。

当社は導入している技術ソリューションとツールを使用して、バックアップの復元テストを定期的に実行しています。

3.3 事業継続性管理（BCM）

Axisにとって、事業継続管理（BCM）は不可欠な要素です。当社では、事業継続を確保するためにさまざまな対策が実施されています。冗長性を確保するため、当社はデータを地理的に異なる場所に所在するプライマリデータセンターとセカンダリデータセンターに保存しています。また、重要度による分類および目標復旧時間（RTO）と目標復旧時点（RPO）の要件に基づいて、資産を資産登録簿に文書化しています。

さらに、事業継続性に影響を及ぼし得る問題が発生した場合に備えて、当社は社内通信における通信計画を施行しています。外部との通信は、status.axis.comのAxisステータスページを通じて管理されています。

3.4 暗号化、鍵、証明書の管理

安全な情報の通信と保存を確保するため、暗号化キーとそれに関連する証明書の適切かつ効果的な使用および管理に関する要件が定義されています。

Axisは、アルゴリズムの選択に関して以下の設定を推奨するFIPS 140-3（IEC/ISO 19790:2012）規格に従っています。

> 移動中のデータの暗号化（TLS / mTLS）- RSA 2048以上
> 保存中のデータの暗号化 - AES 256
> デジタル署名 - RSA 2048以上、ECDSA p256以上、SHA256以上

3.5 アイデンティティとアクセスの管理

アイデンティティとアクセス管理（IAM）とは、論理的資産と物理的資産へのアクセスを承認済みユーザーのみに制限するガバナンスモデルを指しています。予防的観点と検出的観点の両方から、AxisはIAMに関連する多数のセキュリティ制御と実践を実装しています。セキュリティ制御の例として以下が挙げられますが、これらに限定されるものではありません。

> 定義された承認ワークフローによるユーザー登録/登録解除プロセス
> 退職者のActive Directoryアカウントのオフボーディング/無効化の自動プロセス
> 最小権限の原則の適用
> 多要素認証（MFA）
> ユーザーアクセスの定期的な見直し
> ユーザーのアクセスとアクティビティのログ記録と監視
> 特権アカウント管理
> シングルサインオン
> リモートアクセス管理（VPNへのMFAの実装を含む）
> 職務の分離

3.6 インシデント管理

インシデント管理は事業継続性の鍵となるものです。インシデントが発生した場合に備えて、Axisはビジネスと利害関係者への潜在的な影響を最小限に抑えるためのインシデント管理プロセスを定義しています。これには、インシデントを検知、通信、調整、緩和、解決すること、および過去のインシデントから教訓を得て継続的な改善を促進することが含まれます。

Axisは自動ツールを使用してシステムとサービスを積極的に監視することで、異常や潜在的なインシデントの兆候を検知しています。24時間年中無休のインシデント対応体制を強化することを目的として、Axisはセキュリティオペレーションセンター（SOC）を設立しました。SOCは、セキュリティ関連事項を継続的に監視する責任を担っています。また、SOCでは、異常、アラーム、ゼロデイ脆弱性が特定された場合に直ちに対応できる態勢が整っています。

インシデントは、潜在的なビジネスへの影響に基づいて分類されます。そして、適切にエスカレーションされ、解決されるまでインシデント管理システムで追跡されます。すべての主要インシデントについて、インシデントレポートが作成されます。当社は根本原因を突き止めることで、セキュリティ体制の継続的な改善を推進しています。

当社は、プライバシー関連のインシデントや潜在的な侵害をプライバシー侵害管理慣行に従って管理しています。この慣行には、通信チャネル、エスカレーションパス、評価、文書化が含まれます。この慣行は、主にGDPRといった関連プライバシー法や規制に基づいて設定されています。

Axisのサービスに関連するインシデントやステータスに関する外部との通信は、status.axis.comを通じて管理されています。

3.7 IT運用セキュリティ

IT運用セキュリティとは、IT運用環境における機密性、整合性、可用性を保護することを目的としたプロセス、手順、制御を整えることを指します。たとえば、Axisの場合は、クライアントとサーバーの管理、構造化された体系的なプロセスに基づく変更管理の実行、ベストプラクティスとハードニングガイドに従った構成管理の実行がこれに含まれます。

また、IT運用セキュリティにおいて、パッチ管理も重要な一端となります。これは、定義されたライフサイクル管理プロセスの一環として管理されています。

3.8 ネットワークセキュリティ

ネットワーク通信を保護して、確実なアクセスコントロールと運用セキュリティを実現するために、当社はさまざまな対策を実施しています。

セキュリティ制御の例として以下が挙げられますが、これらに限定されるものではありません。

> ロールベースのネットワークアクセス
> 企業ネットワークへのアクセス時における証明書（IEEE 802.1X）の要求
> ネットワークセグメンテーション
> セグメント間の通信におけるファイアウォールポリシー遵守の徹底
> 実稼働ネットワークに接続するクライアントに対するエンドポイント保護の要求
> VPN接続によるリモートネットワークアクセスへの多要素認証の実装
> ネットワークトラフィックとネットワーク機器のプロアクティブな監視
> ネットワーク機器からのログの中央リポジトリへの送信
> ネットワーク機器の変更に関する記録の維持

3.9 人的セキュリティ

人的セキュリティでは、役割に適した人員を選択すること、そして自身の責任に関する従業員と外部関係者（コンサルタントや請負業者）の理解を徹底させることが重要となります。

採用プロセスでは、セキュリティと安全性に関するガイドラインが定義されています。地域の法律や職務の重要性に応じて、これには身元照会や経歴調査が含まれます。

また、このプロセスには、オンボーディング（物理的・論理的アクセスの許可）、秘密保持契約、意識向上とトレーニング、オフボーディング（退職者の物理的・論理的アクセスの終了）など、雇用中および雇用後のセキュリティ対策が含まれます。

3.10 物理的セキュリティ

手順と慣行は、物理的セキュリティを維持すること、Axisの施設における労働者や施設への訪問者全員にとって安全かつ安心できる環境を構築すること、Axisの施設、資産、従業員を保護することを目的として定義されています。

Axisの敷地内に出入りするにはアクセスカードとPINコードが必要です。また、Axisの身分証明書を目立つ場所に着用することが敷地内にいる者全員に義務付けられています。敷地内への立ち入りはすべて記録され、ログが中央リポジトリに送信されます。敷地全体にわたって監視カメラが設置されています。

訪問者は必ずAxis受付で登録し、認められている身分証明書を受付/サービスデスクのスタッフに提示する必要があります。登録を終えた訪問者は常に訪問者バッジを目立つ場所に着用し、Axis敷地内にいる間は常に人員が訪問者に付き添います。

Axisの敷地はさまざまなセキュリティゾーンに分割されており、制限区域への立ち入りは許可を受けている人員に制限されています。

3.11 プライバシー保護

Axisでは、従業員、パートナー、顧客の個人データを保護するための安全対策とメカニズムが完璧に整っています。「信頼性の高い強力なブランド」を戦略の中核に据える当社は、エンドユーザーと透明性の高い関係を築くことに尽力しています。当社はお客様の情報を保持していますが、適用される規制や契約に従って、データ管理に対する個人の完全な権利を常に尊重しています。

個人データの収集と処理に関しては、当社は以下の基本原則を適用しています。

> 公正かつ合法的であること
> 必要な範囲であること
> 正当な目的があること
> 目的に適切である、目的と関連性がある、目的にとって必要であること

当社のプライバシー保護対策に関する詳細については、www.axis.com/privacyを参照ください。

3.12 リモートワーク

Axisは、出張や在宅勤務などのリモートワークで使用されるデバイスを保護するための規則とセキュリティプロセスを定義しています。これはシステムとプロセスを対象としており、業務使用と業務外使用を明確に区別し、安全かつ準拠した方法での作業を徹底することを目的としています。

リモートワークに関する従業員へのガイダンスは、セキュリティ意識向上トレーニングや許容使用ポリシーとして提供されています。オフィス外での作業中に社内システムやリソースにアクセスする各ユーザーは、多要素認証を実装したVPN接続経由で認証を受ける必要があります。

クライアントとモバイルデバイスは暗号化されています。当社は、必要に応じてリモートでデータを消去できる機能を備えたモバイルデバイス管理（MDM）ソリューションを通してモバイルデバイスを管理しています。

3.13 リスク管理

当社は、年間リスク管理サイクルに従って、リスク管理を実施しています。これはセキュリティを含めたすべてのビジネス領域にわたるもので、コーポレートガバナンスによって管理されています。リスク管理サイクルには、リスク評価、リスク分析、リスクフォローアップが含まれます。Axisの経営陣、監査委員会、取締役会にリスク分析が提示されます。

企業のリスク管理サイクルの一環として、情報セキュリティリスク評価ガイドラインが定義され、これがISMSに適用されています。これには、組織全体のシステム責任者とリスク責任者による継続的なリスク評価とリスク軽減対策が含まれます。特定されたリスクは評価され、そのリスクレベルに応じて、リスク評価マトリックスに基づきエスカレーションされます。最高情報責任者（CIO）が経営陣と取締役会へのリスク報告の全体的な責任を担っています。

ISO 27001認証プロセスの一環として、情報セキュリティリスク評価のアプローチ、方法論、実装については、毎年、外部機関による監査を受けています。

3.14 セキュア開発

製品とサービスの安全な開発を確保することを目的として、AxisはAxisセキュリティ開発モデル（ASDM）を定義および実装しています。ASDMの取り組みを推進する主な目的は以下の通りです。

> Axisソフトウェア開発活動にソフトウェアセキュリティを統合すること
> Axisの顧客のビジネスにおけるセキュリティ関連リスクを軽減すること
> 高まりつつある顧客やパートナーのセキュリティ意識に対応すること
> 問題の早期発見と解決により、コスト削減の可能性を創出すること

Axisの製品とソリューションに含まれるすべてのAxisソフトウェアにASDMが適用されます。ASDMの詳細については、help.axis.com/axis-security-development-modelを参照してください。

3.15 セキュリティ意識向上とトレーニング

Axisでは、組織に対するセキュリティの脅威を回避し、軽減するために、従業員を継続的に訓練するセキュリティ意識向上プログラムを開発しています。

意識向上プログラムには、情報セキュリティポリシーと一般的なセキュリティのベストプラクティスに関連するセキュリティ意識向上トレーニングが含まれています。意識向上トレーニングは、Axisの全人員に義務付けられています。

物理的セキュリティに関する安全性とセキュリティのトレーニングも含まれています。Axisの敷地内に出入りするすべての従業員と請負業者にこのトレーニングが義務付けられており、トレーニングを受けなければ敷地内に入るためのアクセスカードを取得することはできません。

組織における役割と責任に応じて、追加のセキュリティトレーニングを課しています。例として、開発者向けのASDMトレーニング（前出のセクション3.14参照）やシステム責任者向けの役割固有の認識向上トレーニングなどが挙げられます。

3.16 システム取得とサプライヤー管理

当社は契約を締結する前に、サプライヤーの精査を実施しています。これには、法的な評価、セキュリティ評価、プライバシー評価が組み込まれている評価モデルに従った潜在的サプライヤーの評価が含まれます。契約マネージャーと法務部門が主にサプライヤー審査を担当しています。また、セキュリティ専門家など、組織内のさまざまな専門家からの助言も得ています。

各サプライヤーには契約責任者が割り当てられます。その責任者が、サプライヤーの納品のフォローアップ、契約要件の履行、定期的なサプライヤーのセキュリティ評価に関する全体的な責任を担います。

Axisの要件に準拠していること、およびAxisや当社パートナーが受け入れ難いリスクに曝されないことを確認するため、調達予定のシステムとサービスには評価が行われます。こうした要件に対応しているのが、システム取得ガイドラインです。新規システムや新規サービスを検討する際には、このガイドラインが必ず適用されます。

3.17 脅威インテリジェンス

脅威インテリジェンスとは、サイバー空間で発生し得る攻撃や有害イベントに対処することを目的として、デジタル脅威や物理的脅威の発生および攻撃者に関する情報を収集し、評価を行うプロセスを指す用語です。

当社は複数の異なるソースを通じて、インテリジェンス分析と脅威インテリジェンスを継続的に実行しています。

Axisはゼロデイ脆弱性を監視するだけでなく、セキュリティコミュニティに参加するなど、脅威情報を積極的に活用することで、脅威インテリジェンスを実現しています。

3.18 脆弱性管理とマルウェア対策

システムやアプリケーションの脆弱性と悪質なコードを評価し、適切なツールと方法論を使用して修復を実施できるように、当社は脆弱性管理とマルウェア対策の手順を定義しています。Axisはさまざまなスキャンツールを活用して、IT環境内外部の脆弱性スキャンを継続的に実行しています。脆弱性はCVSS（共通脆弱性評価システム）に従って分類され、その重大度に基づいて優先順位が付けられます。

実稼働ネットワークに接続するデバイスは、業界をリードするエンドポイント検知・応答ソリューションによって保護および監視されます。

当社製品の脆弱性管理として、製品のライフサイクル全体にわたって、Axisはソフトウェアに Axisセキュリティ開発モデル（前出のセクション3.14参照）を適用しています。AxisはCVE（共通脆弱性識別子）CNA（採番機関）として承認されており、確立されているCVEプログラムフレームワークに従って、高い透明度をもって脆弱性を開示しています。製品のセキュリティと脆弱性管理の詳細については、www.axis.com/support/cybersecurity/vulnerability-management およびhelp.axis.com/axis-vulnerability-management-policyを参照してください。

4. 認定とコンプライアンス

Axisはさまざまな規制要件および戦略的に選択されたフレームワークと標準/規格に準拠しています。このコンプライアンスを貫く姿勢により、Axisとパートナーの両方にとって重要となる情報セキュリティやプライバシーなどの分野に対する当社の取り組みを実証しています。

関連する証明書やコンプライアンスの最新の概要については、以下を参照してください。
www.axis.com/compliance

Axis Communicationsについて

Axisは、セキュリティ、安全性、運用効率、ビジネスインテリジェンスを向上させることで、よりスマートでより安全な世界の実現を目指しています。ネットワークテクノロジー企業として、また業界をけん引するリーダーとして、Axisは映像監視、アクセスコントロール、インターコム、音声ソリューションを提供しています。これらのソリューションは、インテリジェントアプリケーションによって強化され、質の高いトレーニングによってサポートされています。

Axisは50ヶ国以上に5,000人を超える熱意にあふれた従業員を擁し、世界中のテクノロジーパートナーやシステムインテグレーションパートナーと連携することで、カスタマーソリューションをお届けしています。Axisは1984年に創業し、本社はスウェーデン・ルンドにあります。